UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

MOOG INC., Plaintiff, v. SKYRYSE, INC., ROBERT ALIN PILKINGTON, MISOOK KIM, and DOES NOS. 1-50. Defendants.	Civil Action No. 1:22-cv-00187-LJV-JJM

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT SKYRYSE, INC.'S MOTION TO ENTER SOURCE CODE PROTOCOL

I. INTRODUCTION

In its Opposition to Moog's Motion to Compel (ECF 190), Skyryse requested that the Court enter Skyryse's proposed source code protocol, which is updated and attached here as Exhibit A. Moog had ample opportunity to respond, and did respond, in its reply brief (ECF 195). Although that makes a formal cross-motion unnecessary, *see Erickson v. MGM Grand, Inc.*, No. 13 CIV. 564 (NRB), 2014 WL 12774971, at *4 (S.D.N.Y. June 25, 2014), Skyryse submits this motion now at Moog's insistence, and for the Court's full consideration. As explained further below, the existing iDS Protocol (ECF 96-2) was never intended to govern the inspection of any party's own proprietary source code, lacks important restrictions needed to ensure the security of such confidential source code, and adds unnecessary complexity, expense, and risk to the process. Skyryse's source code review protocol, on the other hand, streamlines the issue and reduces risk.

The earlier-entered iDS Protocol addresses the unique situation (inapplicable here) where forensically imaged devices that need to be inspected in discovery contain a *combination* of Moog's and Skyryse's confidential information, and so they are put in the custody of a neutral third party, iDS, to facilitate those inspections. This unprecedented and complex procedure wasn't designed to address the inspection of a single party's proprietary and highly confidential source code, which is what this motion is about. Those sorts of inspections of one party's source code can and should be carried out under the most secure procedures and without the unnecessary involvement of a third party. Only Skyryse's proposed source code protocol is designed for exactly this purpose. It closely follows model source code review protocols routinely ordered by courts around the country in trade secret cases like this, to safely and securely make source code available for review. These security precautions will protect not just Skyryse's source code, but Moog's too.

Skyryse proposed to Moog a reasonable source code review protocol over a month ago, and Moog refused to discuss it. Nonetheless, Skyryse made its source code available for Moog to inspect weeks ago, as long as Moog would abide by Skyryse's source code review protocol, at least provisionally until this dispute was resolved. Still, Moog refused to inspect this source code that it claims to need to review so urgently. Instead of meeting and conferring in good faith, Moog went straight to the Court arguing that under Skyryse's proposed protocol, Moog would be unable to bring anything into the room so it could review Skyryse source code side by side. This is plainly wrong, for nothing in Skyryse's proposed source code protocol prevents a reviewer from bringing documents, such as printouts of its own source code, into the review. Had Moog discussed this issue with Skyryse, it would have understood this, and also learned that Skyryse is open to adjusting its proposed protocol to ensure an inspecting party's counsel and experts can bring paper or electronic copies of their own source code to their inspections, as long as it is done in a safe and secure way. In fact, Skyryse has made exactly this adjustment to its proposal, mooting Moog's concerns.

Moog's refusal to discuss these issues with Skyryse or begin examining the source code typifies Moog's sharp tactics and its preference to litigate about discovery, rather than actually proceeding with it. Only Skyryse's proposed source code protocol sufficiently protects both sides' source code while avoiding the unnecessary risk, burden, and complications that would be imposed by the iDS Protocol if it were now applied to source code inspections. Respectfully, the Court should enter Skyryse's proposed order.

II. THE COURT SHOULD ORDER SKYRYSE'S PROPOSED SOURCE CODE PROTOCOL.

A. Skyryse's source code protocol provides critical security measures not found in the iDS Protocol.

Skyryse's proposed source code protocol includes several necessary protections specific to confidential source code—often a technology company's most prized and sensitive asset—that are noticeably lacking from the iDS Protocol (ECF 96-2). These protections will safeguard not only Skyryse's source code productions, but Moog's too.

First, Skyryse's source code protocol, unlike the iDS Protocol, is actually intended to protect source code, with restrictions on how it is displayed, printed, and otherwise made securely available for inspection with minimal risk. The iDS Protocol, on the other hand, provides a complex, intricate procedure reliant entirely on a third party, and was set up for the narrow circumstance where a forensic device to be made available for inspection contains a mix of Moog and Skyryse information. For those unique instances, the Court saw fit to order that such sensitive material be placed in the custody of a neutral third party, even at significant expense to the litigants. But aside from that unique circumstance where the parties' confidential information is commingled in forensic images, there is no need to involve a third party, and the complications and risks doing so entails, all of which will undoubtedly lead to more issues.

Moog's argument that Skyryse is asking for a "do over" of the parties' dispute over the iDS Protocol is plainly false. July 27 Tr. at 52:11-12. As the briefing made clear, that dispute focused only on discovery of forensic images that commingled both sides' confidential information, not with a single party's information, let alone the inspection of a single party's source code. In fact, the parties' stipulated protective order (ECF 89, ¶8.1) expressly contemplates that they would subsequently negotiate another stipulation to govern the review of their confidential

source code; the iDS Protocol was no such stipulation and was not directed at inspecting the parties' proprietary source code. The parties' earlier dispute over the iDS Protocol and the Court's order resolving it did not address, much less resolve, this dispute over how source code reviews should proceed.

Rule 34 requires that parties make their discoverable information—even their confidential material such as source code—available to the opposing party, but there is no need to make the process more cumbersome or risky by involving a third party. The parties have already faced, and continue to face, considerable challenges and issues in implementing the iDS Protocol where it actually applies to forensic images arguably containing both parties' confidential information. The very involvement and reliance on a third-party vendor complicates the process and makes it more expensive, and iDS has often found itself in the unenviable position of fielding questions and (sometimes conflicting) demands from the litigants, delaying discovery.

Skyryse's source code protocol, on the other hand, keeps each party's source code in the physical custody of its own counsel while allowing it to be thoroughly and privately inspected by the other side, eliminating the risks that would arise if the parties were forced to turn source code over to a third party. If each party's source code were simply turned over to iDS, the parties would effectively lose the ability to monitor and supervise its distribution. Such a requirement is inappropriate and creates unnecessary risks.

Second, only Skyryse's source code protocol allows the producing party the opportunity to approve software the other side intends use to inspect the producing party's source code. Ex. A, ¶4.3(e). This is essential to ensuring that no party, even inadvertently, puts confidential source code at unnecessary risk of disclosure. For example, under the iDS Protocol, which unquestionably allows for internet access, Moog has already installed standard web browsers, through which one

could make source code available over the Internet. While the iDS Protocol attempts to partially restrict internet access, it does so by requiring the parties rely entirely on iDS to create a flawless system. Conversely, Skyryse's protocol avoids that risk by eliminating unnecessary Internet access entirely, while still allowing a full inspection of the source code on a dedicated stand-alone computer, equipped with appropriate source code review tools. Ex. A, ¶4.3(b) ("All Source Code shall be made available for inspection in a secure room on a secured computer without Internet access or network access to other computers and on which all access ports have been disabled.").

Third, Skyryse's source code protocol prohibits any party from printing more of its adversary's source code than necessary without cause, eliminating the risk that unlimited blocks of proprietary, confidential source code can be printed on paper and walked out of the room. Under both the iDS Protocol and Skyryse's proposed source code protocol, the reviewing party may request printouts of portions of source code (for example, for putting excerpts into court filings or experts reports). But unless the scope of these printouts is limited, nothing would prevent someone under the iDS Protocol from printing out an adversary's *entire codebase* and taking it to an unsecure location, undermining the whole purpose of a restrictive review process.

Putting reasonable limits on the printing of code, as only Skyryse proposes, significantly reduces that risk, while allowing the parties to print the excerpts they need. For that reason, Skyryse's source code protocol places common-sense and customary limits both on consecutive pages (10) and total pages (100) that may be requested to be printed, beyond which any requests are presumptively excessive. Ex. A, ¶4.3(g). The iDS Protocol, which again applies to a different category of discoverable material, does this in reverse: any and all requests for printouts are presumptively approved regardless of their scope or length, and the burden is on the producing party to show excess. Moreover, Skyryse's source code protocol also ensures that any printouts of source

code are kept in a secure location and in a secure manner, a common practice for maintaining source code printouts. Ex. A, ¶3.1. The iDS Protocol lacks even this basic restriction.

Fourth, while both the iDS Protocol and Skyryse's source code protocol allow reviewers to take notes, only Skyryse's source code protocol prohibits reviewers from copying source code into their notes. Ex. A, ¶4.3(f). This again protects source code by limiting the number of ways it may be inadvertently disclosed. Conversely, the iDS Protocol allows reviewers to include whatever they like in the notes (just so long as the notes are not used to recreate the materials for outside use). While this may be sufficient for normal document inspections, it creates unnecessary risk for sensitive source code.

These representative examples are just a few of the ways that the iDS Protocol is deficient and inappropriate for source code review, and Skyryse's source code protocol provides necessary protections that will benefit both sides. The iDS Protocol, aimed at addressing the unique and specific need for the inspection of forensic devices with a mix of both Moog and Skyryse information, is insufficient to adequately protect the production of source code reflecting just one party's proprietary information.

B. Skyryse's source code protocol is based on model orders used by courts around the country, unlike the iDS Protocol, which is unprecedented.

Skyryse's source code protocol, unlike the iDS Protocol, is modeled after standard source code review protocols routinely entered in trade secret cases across the country. For example, Skyryse's source code protocol contains many of the source code protections in the "Model Protective Order for Litigation Involving Patents, Highly Sensitive Confidential Information ***and/or Trade Secrets***" provided by the court in the Northern District of California. https://www.cand.uscourts.gov/forms/model-protective-orders/. That model protective order, like Skyryse's proposal, is *not* used only in patent cases, as Moog's counsel has intimated. That court

and others around the country routinely enter similar protective orders in trade secret cases involving source code.

Both Skyryse's source code protocol and the Northern District of California's model order provide that source code will be made available for inspection on a secure computer in a secure room without internet access. These secure computers are hosted and maintained by the producing party's counsel to ensure the security of the source code. Making source code available for inspection on a stand-alone computer without internet access is the norm in trade secret cases across the country. *See, e.g.*, *Virgilant Techs. Ltd. v. ABC Assets, Inc.*, Dkt #61, 1:21-cv-00181-MN (D. Del. June 23, 2022); *Hullinger v. Anand*, 2:15-cv-07185-SJO-FFM, Dkt #238 (C.D. Cal. June 30, 2016); *Lithero, LLC v. AstraZeneca Pharm. LP*, 1:19-cv-02320-RGA, Dkt #93 (D. Del. Feb. 22, 2021); *ResMan, LLC v. Karya Prop. Mgmt, LLC*, 4:19-cv-00402-ALM, Dkt #24 (E.D. Tex. June 17, 2019); *Carolina Coupon Clearing, Inc. v. Cardinal Health Managed Care Servs.*, LLC, 1:16-cv-00412-WO-JEP, Dkt #163 (M.D.N.C. Feb. 16, 2017); *Level One Techs., Inc. v. Penske Truck Leasing Co., L.P.*, 4:14-cv-01305-ROW, Dkt #57 (E.D. Mo., Feb. 23, 2016); *T.N. Inc. Ltd. v. Fidelity Nat'l Info. Servs., Inc.*, 2:18-cv-05552-WB, Dkt #85 (E.D. Pa. Sept. 4, 2020); *Crowdstrike, Inc. v. NSS Labs, Inc.*, 1:17-cv-00146-MN, Dkt #53 (D. Del. Apr. 3, 2018). Each of the foregoing protective orders provides substantially the same protections as Skyryse's source code protocol, and provides the parties ample opportunity to examine and inspect source code for even very subtle copying.

Conversely, Courts are reluctant to impose burdensome protocols on litigants beyond what is included in standard source code review protocols—especially when the alternative would add risk, burden, and expense. *Kelora Sys., LLC v. Target Corp.*, No. C 10-04947 CW LB, 2011 WL 6000759, at *3 (N.D. Cal. Aug. 29, 2011) ("[A] departure from the district's model protective

order is unwarranted because the benefits of making it easier for [plaintiff] to evaluate the [defendant's] source code do not outweigh the burdens associated with the proposal."). "[D]iscovery is intended to ensure that the requesting party has the information necessary to make its case but this does not imply that the requesting party may force the producing party to undertake burdensome measures merely for the convenience of the requesting party." *Id*.

While the iDS Protocol may be more convenient for Moog, it was never intended to apply to either side's source code, whereas a standard and more secure source code review protocol as Skyryse has proposed is more than sufficient to allow Moog to try to make its case. *See Dynetix Design Sols., Inc. v. Synopsys, Inc.*, C-11-05973 PSG, 2012 U.S. Dist. LEXIS 51724 at *5-9 (N.D. Cal. Apr. 12, 2012) (rejecting plaintiffs' requested departure from the model protective order where plaintiff "may have shown that it will be more difficult to manage the case if it must review source code at opposing counsel's offices or another agreed upon location, however, the court is not convinced that this would significantly prejudice [plaintiff's] presentation").

C. Skyryse's source code has been available to Moog for weeks.

Skyryse's source code has been available for Moog to inspect for the last three weeks at counsel's offices in Silicon Valley, yet Moog has refused to look at it. Skyryse even told Moog it would set up a review computer in any other city where Skyryse's counsel have offices (e.g., New York, Los Angeles, San Francisco, where Moog's counsel also have offices) if that would be more convenient for Moog, but Moog refused to discuss it. So any delay of which Moog complains is of its own making. Moog could have started reviewing Skyryse's code long ago by simply agreeing, even provisionally, to abide by the security protections in Skyryse's proposed source code review protocol. But Moog refused, preferring to litigate the issue while deliberately choosing not to review Skyryse's source code in the meantime. This is not the behavior of a party legitimately interested in discovery and in need of some urgent, emergency relief.

D. Skyryse's proposed protocol readily allows for counsel and experts to compare the parties' code with reasonable restrictions.

Moog has refused to even discuss Skyryse's proposed protocol, and instead, at the July 27 hearing, Moog sprung on Skyryse the argument that Moog could never compare its source code to Skyryse's because Skyryse's source code protocol purportedly "did not permit [Moog] to bring anything into the [review] room," claiming it "is impossible for us to bring anything in." July 27 Tr. at 49:13-18. This is wrong.

First, Moog ignores that there are dozens of volumes of electronically stored information—including some portions of Skyryse source code—available for it to inspect under the iDS Protocol already. For each device or repository that a party turned over to iDS because it might arguably contain a mix of both Moog's and Skyryse's confidential information (and there are dozens of such forensic images in iDS's custody), the iDS Protocol already allows Moog's lawyers and experts to compare these devices and repositories side-by-side with any other device or repository in iDS's possession. But this is not enough for Moog, which now wants the Court to apply the iDS Protocol to the inspection of *other* repositories of Skyryse's proprietary source code, even code that does not contain a mix of both sides' confidential information. Moog has made no showing why this same approach is necessary or makes any sense when applied to Skyryse's own proprietary source code.

Second, and contrary to Moog's statements at the hearing, nothing in Skyryse's source code protocol prevents the parties' counsel or experts from bringing documents such as printouts of their own client's source code into the room during the inspection of their adversary's source code. *See* Ex. A, ¶4.3(c). To the contrary, the protocol even addresses how to deal with documents inadvertently left in the room after review. *See id*., ¶4.3(j). If Moog had simply met and conferred with Skyryse about the issue before rushing the dispute to the Court, Skyryse would have pointed

out that Moog was mistaken on this. Conversely, if Moog felt the source code protocol needed some revision to even more explicitly state that Moog's lawyers and experts could bring Moog's own source code with them during an inspection, Skyryse would have been open to discussing this. In fact, to moot Moog's concern, Skyryse has adjusted its proposal to make clear that an inspecting party *can* bring a copy of its own source code to an inspection, following a simple procedure that does not risk the security of the code being inspected. Ex. A, ¶4.3(c).

E. Moog is abusing the iDS Protocol.

Moog seeks to extend the iDS Protocol in a way that was never intended and that the Order does not permit. The parties' March 11 Stipulation states that the only materials to be turned over to iDS are those which "necessarily include[] property of any Defendant" mixed with Moog's information. (ECF 25 at 2.) Despite this clear mandate, Moog has instead produced to iDS, and *not* to the Defendants directly, Moog-only information including source code, which in practice means it now can only be inspected through the iDS Protocol. At first, Skyryse did not understand why Moog would do this, but Moog's recent positions have made its intentions clear.

If Moog is successful in getting the Court to compel Skyryse to turn over its own Skyryse-only proprietary source code to iDS too, then under the iDS Protocol—which has few of the restrictions typically found in source code review orders—Moog will have virtually unfettered access to Skyryse's code, and can run automated comparisons of Moog's code to Skyryse's on a single review computer. This, despite Moog having made no showing that the Skyryse code at issue "necessarily includes" anything belong to Moog. This was never contemplated or authorized by the March 11 Stipulation or the iDS Protocol. Worse, it all but ensures that Moog will root around in Skyryse's code—despite no indication that it contains any Moog information—looking for any similarities to Moog's code (and like any two code bases, they are likely to share at least

certain programming conventions and syntax) to spin as "trade secrets," or to take credit for Skyryse's innovations.

III. CONCLUSION

At bottom, only Skyryse's source code protocol allows the parties to safely and securely inspect source code under a procedure that applies standard, common-sense restrictions used by other courts in trade secret cases across the country. Conversely, the highly idiosyncratic and unprecedented iDS Protocol—which on its face does not apply to a party's source code that does not "necessarily include" the other side's information—would unnecessarily expose the parties' most sensitive assets to a third party when there is no reason to do so, and is certain to cause more complications, delays, and expense. Skyryse's source code protocol streamlines the process for securely inspecting source code; the iDS Protocol complicates and delays it, makes it more expensive and adds risk. Skyryse respectfully requests that its proposed source code protocol be ordered by the Court.

Dated: August 3, 2022

/s/ Gabriel S. Gross

LATHAM & WATKINS LLP

Douglas E. Lumish (Admitted *Pro Hac Vice*)
Gabriel S. Gross
Arman Zahoory (Admitted *Pro Hac Vice*)
Ryan Banks (Admitted *Pro Hac Vice*)
140 Scott Drive
Menlo Park, California 94025
Telephone: (650) 328-4600
Facsimile: (650) 463-2600
Email: doug.lumish@lw.com
gabe.gross@lw.com

Joseph H. Lee (Admitted *Pro Hac Vice*)
650 Town Center Drive, 20th Floor
Costa Mesa, California 92626
Telephone: (714) 540-1235

Facsimile: (714) 755-8290
Email: joseph.lee@lw.com

Julianne C. Osborne (Admitted *Pro Hac Vice*)
505 Montgomery Street, Suite 2000
San Francisco, CA 94111
Telephone: (415) 391-0600
Fax: (415) 395-8095
Email: julianne.osborne@lw.com

HARRIS BEACH PLLC
Terrance P. Flynn
726 Exchange Street, Suite 1000
Buffalo, New York 14210
Telephone: (716) 200-5050
Email: tflynn@harrisbeach.com

Counsel for Defendant Skyryse, Inc.